LISTING OF CLAIMS

1. (currently amended) A method for prohibiting access to a computer, having a radio frequency identification (RFID) chip, after a radio frequency antenna security device has been removed from said computer, comprising the steps of:

(a) storing data comprising at least an antenna history bit indicating that said security device was originally attached to said computer in a first region of first storage means in said computer;

(b) starting a procedure for prohibiting the access to change said stored data at said computer following the completion of said step (a);

(c) using said data stored in said first region to verify that said security device was once attached to said computer;

(d) dynamically determining that said security device is no longer attached to said computer; and

(e) prohibiting the access to said computer in response to said steps (c) and (d).

2. (original) The method according to claim 1, wherein said step (b) is initiated in response to a trigger event.

3. (original) The method according to claim 1, wherein said step (e) is performed only when an authorized password is not entered.

4. (previously presented) The method according to claim 3, further comprising the step of:

storing, in response to receipt of an authorized password, data indicating that said security device that was once attached to said computer has been removed in a second region of said first storage means.

5. (canceled)

6. (currently amended) A method for prohibiting access to a computer, having a radio frequency identification (RFID)

chip, after a radio frequency antenna security device has been removed from said computer, comprising the steps of:

(a) storing data comprising at least an antenna history bit indicating that said security device was once attached to said computer in a first region of first storage means in said computer;

(b) permitting a central processing unit in said computer to monitor periodically to determine whether said security device is still attached to said computer; ~~and~~

(c) determining if an authorized password has been entered;

(d) permitting access to said computer when an authorized password has been entered; and

(e) prohibiting the access to said computer in response to said step (b) when it is determined that an authorized password has not been entered.

7. (currently amended) A computer, having a radio frequency identification (RFID) chip, capable of having a

radio frequency (RF) antenna security device removably installed therein, comprising:

first storage means at said RFID chip capable of storing data received from said RF antenna while a main power source of said computer is turned off;

a central processing unit; and

second storage means storing a program that permits said computer to perform the steps of:

(a) storing data comprising at least an antenna history bit indicating that said security device was once attached to said computer in a first region of the first storage means in said computer;

(b) starting a procedure for prohibiting access to change said stored data in said computer following the completion of said step (a);

(c) using said data stored in said first region to detect that said security device was once attached to said computer;

(d) detecting that said security device has been removed from said computer; and

(e) prohibiting the access to said computer in response to said steps (c) and (d).

8. (previously presented) The computer according to claim 7 wherein the second storage means additionally permits the computer to perform the steps of determining whether removal of said security device was authorized, and storing, in response to said determination data indicating that said security device that was once attached to said computer has been legitimately removed in a second region of said first storage means.

9. (currently amended) A computer, having a radio frequency identification (RFID) chip, capable of having a radio frequency (RF) antenna security device removably installed therein, comprising:

first storage means at said RFID chip capable of storing data received from said RF antenna while a main power source of said computer is turned off;

a central processing unit; and

second storage means storing a program that permits said computer to perform the steps of:

(a) storing data comprising at least an antenna history bit indicating that said security device was once attached to said computer in a first region of the first storage means in said computer;

(b) causing the central processing unit in said computer to periodically monitor to determine whether said security device has been removed from said computer; and

(c) prohibiting access to said computer in response to a determination in step (b) that the security device has been removed.

10. (currently amended) A computer, having a radio frequency identification (RFID) chip, capable of having a radio frequency (RF) antenna security device removably installed therein, comprising:

first storage means at said RFID chip capable of storing data received from said RF antenna while a main power source of said computer is turned off;

a central processing unit;

means for storing data comprising at least an antenna history bit indicating that said security device was attached to said computer in a first region of the first storage means;

first detection means for using said data stored in said first region to detect that said security device was once attached to said computer;

second detection means for detecting that said security device has been removed from said computer; and

means for prohibiting access to said computer in response to said detection means.

11. (previously presented) The computer according to claim 10 further comprising means for determining if removal of said security device was authorized and means for storing, in response to said determination data indicating that said security device that was once attached to said computer has been legitimately removed therefrom in a second region of said first storage means.

12. (currently amended) A computer, having a radio frequency identification (RFID) chip, capable of having a radio frequency (RF) antenna security device removably installed therein, comprising:

first storage means at said RFID chip capable of storing data received from said RF antenna while a main power source of said computer is turned off;

a central processing unit;

means for storing data comprising at least antenna history, antenna error, detect coil, detect enable, tamper and access protection bit regions indicating that said security device that was once attached to said computer has been removed therefrom in a region of the first storage means;

detection means for using said data stored in said region to detect that said security device attached to said computer has been removed therefrom; and

means for prohibiting, in response to said detection means, access to said computer.

13-20 (canceled)

21. (original) The computer according to claim 14, wherein said RF antenna is attached to a lid of a device bay of said computer.

22. (original) The computer according to claim 15, wherein said RF antenna is attached to a lid of a device bay of said computer.

23. (original) The computer according to claim 16, wherein said RF antenna is attached to a lid of a device bay of said computer.

24. (original) The computer according to claim 17, wherein said RF antenna is attached to a lid of a device bay of said computer.

25. (original) The computer according to claim 18, wherein said RF antenna is attached to a lid of a device bay of said computer.

26. (original) The computer according to claim 19, wherein said RF antenna is attached to a lid of a device bay of said computer.

27. (canceled)

28. (previously presented) The method according to claim 1 wherein said storing is done in response to receipt of an RF excitation signal received from a remote RF transmitter.

29. (previously presented) The method according to claim 6 wherein said storing is done in response to receipt of an RF excitation signal received from a remote RF transmitter.

30. (previously presented) The method according to claim 6 further comprising, upon determining that an authorized password has been entered, storing in a second region of said first storage means additional data indicating that said security device that was once attached to the computer has been legitimately removed.